Sniper Forensics.
Introduction.
Introduction.

Lee Sult: CTO and Cofounder of Horangi

- Trustwave SpiderLabs
- Palantir
- CISSP
- GCIH
- Investigator of Bad Dudes!

* Disclaimer: IANAL (I am not a Lawyer)
Agenda.
Schedule:

1. Components of an Attack
2. Why an Investigation?
3. Mitigating Risk
Components of an Attack.
Components of an Attack.

This is commonly referred to as the “Breach Quad”- term credited to Colin Sheppard, Director of IR at FIS.
Why an Investigation
Quantifying Risk

Basically Three Questions:

– When did they get in?
– How long were they there?
– Which systems/data were impacted?
Quantifying Risk

4 total systems
100 thousand credit cards
Only 2 systems compromised
Only 50 thousand at risk
Mitigating Risk.
Types of Risk?

Regulatory
Operational
Reputational
(Boils down to Financial Risk)
What to Do?

Contracts
Insurance
Security Controls
Investigations
Questions?
Thank you!